ATACURI PRIVIND SECURITATEA REŢELEI STUDIU DE CAZ – ARP POISONING

Luminița DEFTA, *Student Doctorand, Universitatea din Piteşti*

ABSTRACT: *ARP poisoning este unul dintre cele mai întâlnite atacuri dintr-o rețea comutată. Un switch reprezintă un dispozitiv de rețea care limitează capacitatea atacatorilor ce folosesc un packet sniffer de a obține informații din rețeaua internă. Totuşi, folosind ARP poisoning, traficul dintre două calculatoare poate fi interceptat chiar şi într-o rețea care foloseşte switch-uri. Această metodă este cunoscută ca atacul omului din mijloc. Prin acest tip de atac, stațiile afectate dintr-o rețea vor ajunge să aibă intrări eronate în tabela ARP. Astfel, aceasta va conține doar corespondența dintre adresa IP a stațiilor din aceeaşi rețea şi o singură adresă MAC (cea a stației care a inițiat atacul).*

In această lucrare vom prezenta pas cu pas inițierea unui astfel de atac într-o rețea formată din trei calculatoare. Vom intercepta traficul dintre două stații folosindu-ne de cea de-a treia (a atacatorului).

CUVINTE CHEIE*: rețea, securitate, atacuri, arp poisoning, mac.*

1. Introducere

Într-o rețea de calculatoare este foarte important ca informațiile transmise să nu poată fi accesate sau interceptate de către persoane neautorizate. Acest aspect este esențial în condițiile în care rețelele de calculatoare au ajuns să fie folosite inclusiv pentru realizarea de operațiuni bancare.

Unul dintre atacurile prin care se poate intercepta traficul dintre două calculatoare din aceeaşi rețea este ARP poisoning. Din păcate este greu detectabil şi uşor de folosit în rețelele locale actuale.

2. Ce reprezintă ARP?

ARP reprezintă Address Resolution Protocol. Scopul acestui protocol este acela de a permite fiecărui sistem din rețea să-şi

NETWORK SECURITY ATTACKS. ARP POISONING CASE STUDY.

Luminița DEFTA, *Ph.D Student, University of Piteşti*

ABSTRACT: *Arp poisoning is one of the most common attacks in a switched network. A switch is a network device that limits the ability of attackers that use a packet sniffer to gain access to information from internal network traffic. However, using ARP poisoning the traffic between two computers can be intercepted even in a network that uses switches. This method is known as man in the middle attack. With this type of attack the affected stations from a network will have invalid entries in the ARP table.*

Thus, it will contain only the correspondence between the IP addresses of the stations from the same network and a single MAC address (the station that initiated the attack). In this paper we present step by step the initiation of such an attack in a network with three computers. We will intercept the traffic between two stations using the third one (the attacker).

KEY-WORDS*: network, security, attacks, arp poisoning, mac.*

1. Introduction

In a computer network is very important to not allow the unauthorized persons to gain access to the information sent between computers. This aspect is essential given the fact that the computer networks are used today for many banking operations.

One of the attacks that can intercept the traffic between two computers from the same network is ARP Poisoning. Unfortunately it is hard to detect and very easy to use in the existing local networks.

2. What is ARP?

ARP means Address Resolution Protocol. The purpose of this protocol is to allow each system from the same network to build a table of mappings between the IP and MAC

construiască o tabelă de mapări între adresele de IP şi cele fizice. Acest set de mapări este cunoscut sub numele de ARP cache sau tabela ARP.

Dacă un sistem doreşte să transmită un pachet către un alt sistem aflat în aceeaşi reţea, acesta va verifica în primul rând tabela ARP. Dacă nu este gasită maparea dorită, sistemul va trebui să invoce protocolul ARP şi va face acest lucru prin transmiterea unei cereri ARP prin reţea (prin difuzare). Această cerere conţine adresa IP dorită. Fiecare sistem receptionează această cerere şi verifică dacă se potriveşte cu propria adresa IP. Dacă se potriveşte, sistemul implicat va trimite un mesaj de răspuns care conţine adresa de nivel legatură de date. Sursa cererii va adăuga şi această informaţie în propria tabelă ARP.

Există două tipuri de înregistrări ARP: *statice* şi *dinamice*. De cele mai multe ori, se folosesc intrările dinamice ARP. Asta înseamnă că înregistrarea ARP (MAC-IP) este păstrată pe un dispozitiv atât timp cât acesta este utilizat. O înregistrare statică ARP presupune introducerea manuală a legăturii dintre adresa MAC şi adresa IP.

Cache-ul ARP poate fi vizualizat prin folosirea comenzii ‚arp –a' din linie de comandă. Ieşirea comenzii va fi asemănătoare cu cea de mai jos:

addresses. This set of mappings is known as the ARP cache or ARP table.

If a system wants to send a packet to another system from the same network, it will first check the ARP table. If the desired mapping is not found, the system will send a broadcast ARP request. This request contains, among other things, the desired IP address. Each system receives this request and sees if it matches with its own IP address. If it fits, the involved system will send a reply message containing the data link layer address (MAC). The requester will add this information in its own ARP table.

There are two types of ARP entries: static and dynamic. Most time, the dynamic ARP entries are used. This means that the ARP (MAC – IP) entry is stored on a device as long as it is used. A static ARP record requires the manual entry of the link between the MAC and IP address.

We can view the ARP cache by running the 'arp -a' command. The output will be similar to the one below:

Internet Address	Physical Address	Type
192.168.1.1	00-1d-6a-94-82-89	dynamic
192.168.1.3	00-0c-29-73-4b-c2	dynamic
192.168.1.4	00-0c-29-76-64-3d	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.12	01-00-5e-00-00-0c	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

3. Scurtă descriere a atacului

Atacul ARP poisoning redirecţionează traficul dintre orice staţie din reţeaua locală şi routerul de ieşire din LAN (gateway) prin staţia atacatorului. Acest lucru este realizat prin trimiterea de pachete ARP (atât cereri cât şi răspunsuri) cu informaţii alterate.

Ca exemplu, să presupunem că avem trei calculatoare (W1, W2 si W3), iar unul dintre ele (W1) doreşte interceptarea traficului dintre W2 si W3.

Configuraţia tabelei ARP dinaintea atacului este următoarea:

Atacatorul (W1)
IP: 192.168.1.2
MAC: A4-BA-DB-D8-1F-6E
Prima victima (W2)
IP: 192.168.1.3
MAC: 00-0C-29-73-4B-C2
A doua victima (W3)
IP: 192.168.1.4
MAC: 00-0C-29-76-64-3D

Staţia W1 va trimite două pachete ARP de tip răspuns fals: o dată pentru staţia W2 în care se specifică că adresă MAC a staţiei W3 este A4-BA-DB-D8-1F-6E, şi o dată pentru staţia W3, în care se specifică faptul că adresa MAC a staţiei W2 este tot A4-BA-DB-D8-1F-6E. Astfel, atunci când staţia W3 doreşte să transmită un pachet staţiei W2, îl va transmite staţiei W1. La fel, atunci când staţia W2 doreşte să transmită un pachet staţiei W3, îl va transmite tot staţiei W1.

Pentru ca procesul să funcţioneze, staţia W1 va trebui să trimită pachetele primite staţiilor care sunt adresate. În plus, W1 trebuie să retrimită pachetele ARP false la intervale regulate. Aceasta pentru că intrările din tabela ARP sunt evacuate după un timp, caz în care staţia va trimite un pachet ARP de interogare. Dacă staţia interogată răspunde, intrarea din tabela ARP

3.A brief description of the attack

The ARP poisoning attack redirects the traffic between any station from the local network and the output router (gateway) through the attacker station. This is done by sending ARP packets (both requests and replies) with altered information.

For example, let's suppose we have three computers (W1, W2 and W3) and one of them (W1) wants to intercept the traffic between W2 and W3.

The ARP table configuration before the attack is the following:

The attacker (W1)
IP: 192.168.1.2
MAC: A4-BA-DB-D8-1F-6E
First victim (W2)
IP: 192.168.1.3
MAC: 00-0C-29-73-4B-C2
Second victim (W3)
IP: 192.168.1.4
MAC: 00-0C-29-76-64-3D

The W1 station will send two false ARP packets as response: the first one for the W2 station which specifies that the MAC address of the station W3 is A4-BA-DB-D8-1F-6E and the second for the W3 station which specifies that the MAC address of the station W2 is again A4-BA-DB-D8-1F-6E.

Thus, when the W3 station wants to send a packet to the W2 station, it will transmit it to the W1 station. Similarly, when the W2 station wants to send a packet to the W3 station, it will transmit it to the same W1 station.

For the process to work, the W1 station will have to send the incoming packets to the target stations. In addition, W1 must resend the false ARP packets at regular intervals. This because the ARP table entries are released after a while, in which case the station will send an ARP query packet. If the interrogated station responds, the corresponding ARP table entry will be updated and the traffic will not reach to the W1.

4.ARP poisoning in practice

va fi actualizată şi traficul nu va mai ajunge la W1.

4. ARP poisoning în practică

Pentru a pune în practică un astfel de atac vom folosi utilitarul Cain & Abel disponibil la adresa http://www.oxid.it/cain.html. Vom încerca să interceptăm traficul dintre staţiile W2 şi W3 cu ajutorul staţiei W1 (atacatorul). Pentru simularea reţelei vom folosi o staţie fizică (W1 cu Windows 7) şi două maşini virtuale (W2 cu Windows Server 2003 şi W3 cu Windows XP).

Arhitectura reţelei folosite este redată mai jos în figura 1:

To put in practice such an attack we will use the Coin & Abel utility available at http://www.oxid.it/cain.html. We'll try to intercept the traffic between the W2 and W3 stations using the W1 station (the attacker). To simulate the network we'll use a physical station (W1 with Windows 7) and two virtual machines (W2 with Windows Server 2003 and W3 with Windows XP).

The network architecture is shown below:

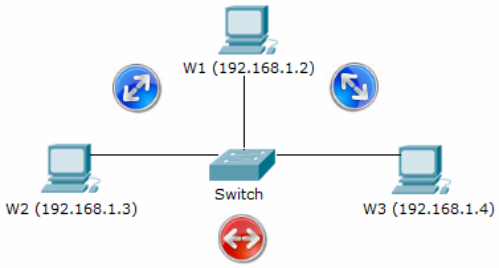

Fig. 1 – Structura reţelei (The Network Structure)

Înainte de iniţierea acestui atac, vom configura anumiţi parametri ce vor ajuta în descoperirea staţiilor din reţea şi în deciderea asupra căror staţii se va lansa atacul.

Primul pas îl reprezintă pornirea snifferului şi alegerea plăcii de reţea pe care se va începe capturarea pachetelor. Pentru alegerea plăcii de reţea vom selecta opţiunea ‚Configure', iar pornirea snifferului se realizează prin apăsarea butonului ‚Start/Stop Sniffer', ca în figura 2 de mai jos:

Before the attack initiation, we'll configure some parameters that will help us to discover the network stations and to decide on which stations we'll launch the attack.

The first step is to start the sniffer and then to choose the network card used to intercept the packets. To choose the network card we'll select the 'Configure' option, and the starting of the sniffer is done by clicking the 'Start/Stop Sniffer' button, as shown below:

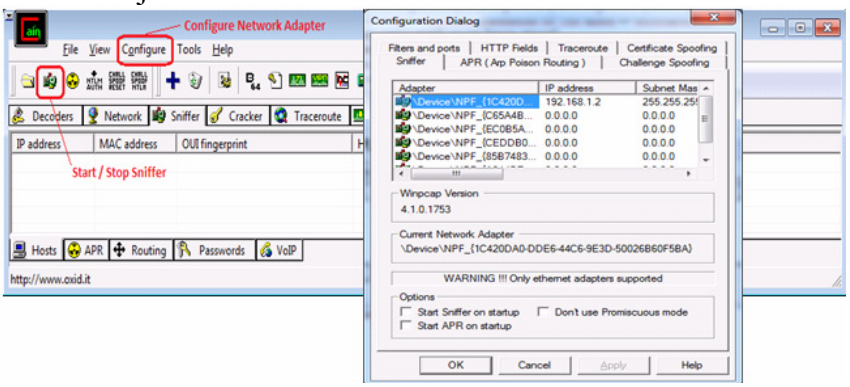

Fig 2. – Network Card Selection / Sniffer Start

După pornirea snifferului ar trebui să descoperim staţiile din reţea. Pentru ca pachetele capturate să poată fi rutate către destinaţia corectă, trebuie să cunoaştem asocierile dintre IP şi MAC ale staţiilor din reţea. Acest lucru se poate realiza prin alegerea tabului ‚Sniffer' click dreapta în fereastra asociată şi alegerea opţiunii ‚Scan Mac Addresses', apoi bifarea opţiunii ‚All hosts in my subnet'.

În cazul reţelei noaste rezultatul este afişat în figura 3.

Observăm că au fost detectate staţiile 192.168.1.1 (default gateway), 192.168.1.3 (W2) şi 192.168.1.4 (W3) cât şi adresele lor MAC asociate.

Pentru a selecta staţiile asupra cărora se va lansa atacul se alege din bara de jos tab-ul APR şi apoi butonul ‚+' din bara de sus ca în figura 4.

After starting the sniffer we have to find the remote computers. To route the captured packets to the correct destination, we must know the correspondence between the IP and the MAC addresses of the network stations. This can be achieved by choosing the 'Sniffer' tab, right click in the associated window, then selecting the 'Scan Mac Addresses' with the 'All hosts in my subnet' option checked.

For our network, the result is shown in the figure 3.

We can observe that the following stations were detected: 192.168.1.1 (default gateway), 192.168.1.3 (W2) and 192.168.1.4 (W3) and also their associated MAC addresses.

To select the target stations, we must choose from the bottom pane the 'APR' tab and then click the '+' button from the top pane like in the figure 4.

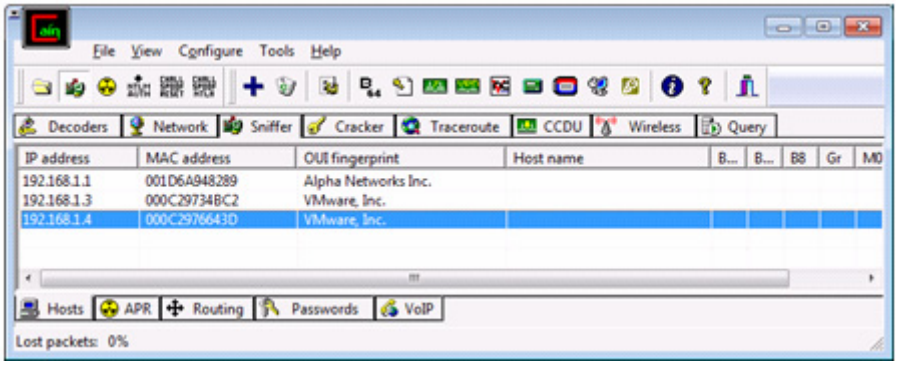

Fig 3. – Network Scan Result

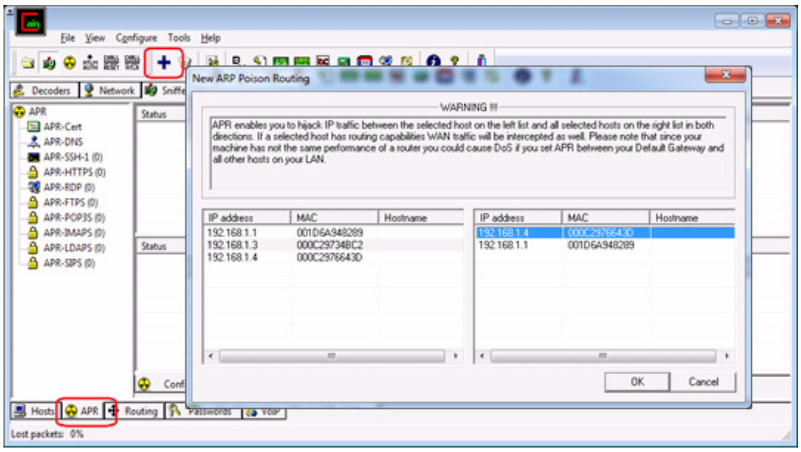

Fig 4. Choose the victim stations

Traficul va fi interceptat în ambele

The traffic will be intercepted in both directions

direcţii între staţia cu IP-ul 192.168.1.3, aleasă din partea stangă şi staţia cu adresa 192.168.1.4 selectată în partea dreaptă. Atacul poate fi lansat acum prin simpla apăsare a butonului APR.

Din figura 5 se observă contorizarea pachetelor ce trec prin staţia atacatorului precum şi direcţia în care sunt rutate.

Dacă pachetele nu sunt rutate către destinaţia corectă, numerele din coloanele Packets nu sunt egale, putându-se crea astfel un atac DoS (Denial of Service) pentru staţiile victimă, dar care este uşor detectabil. Un astfel de atac poate bloca reţeaua prin inundarea acesteia cu trafic inutil.

Există posibilitatea ca atacul să se încheie cu success doar pentru una dintre staţii. Acest lucru se poate întâmpla spre exemplu dacă o staţie are definite intrări ARP statice. Astfel se va observa că numărul pachetelor rutate vor creşte doar într-o singură direcţie, snifferul prelucrând doar o parte din traficul aşteptat.

Deoarece intrările dintr-o tabelă ARP expiră, Cain & Abel trimite pachete ARP false la fiecare 30 de secunde, timp ce poate fi modificat din meniul Configure. Dacă se doreşte ascunderea identităţii atacatorului, se poat seta tot de aici şi adresele IP şi MAC sursă (vezi fig. 6).

between the station with the 192.168.1.3 IP, chosen from the left side, and the station with the 192.168.1.4 address, selected from the right side. The attack can be launched now by simply pressing the APR button.

From the figure 5 we can observe the counting of the packages which pass through the attacker station and also the direction in which they are routed.

If the packets are not routed to the correct destination, the numbers from the 'Packets' columns are not equal, and thus can create a DoS (Denial of Service) attack for the victim stations, but which is easily detectable. Such an attack can block the network by flooding it with useless traffic.

There is the chance that the attack to succeed only for some of the target stations. This can happen for example if a station has static ARP entries defined. Thus, we can observe that the number of the routed packets will grow only in one direction, the sniffer processing only a part of the expected traffic. Because the ARP table entries expires after a while, Cain & Abel sends fake ARP packets at every 30 seconds, time which can be modified from the 'Configure' menu. If we want to hide the identity of the attacker we can set here also the source IP and MAC addresses using the 'Use Spoofed IP and MAC addresses' option (see figure 6).

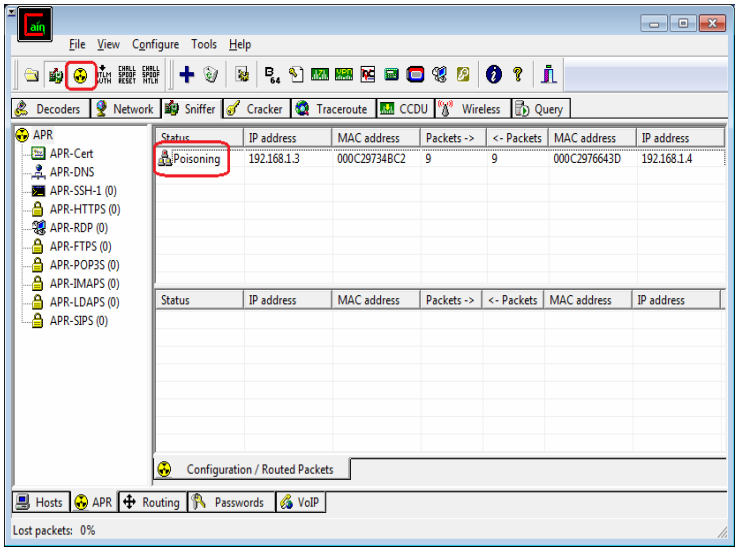

Fig. 5 - Starting the attack

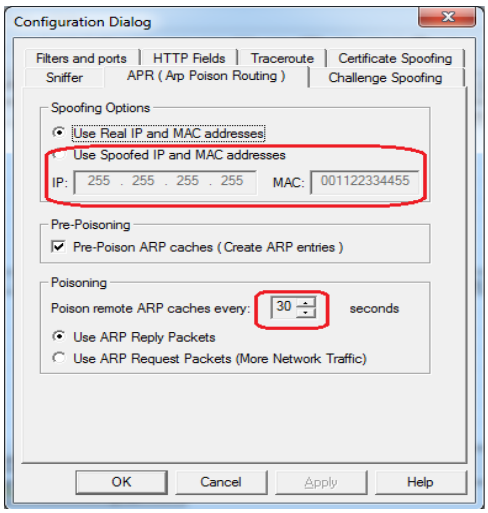

Fig 6 – Configure advanced parameters

Capturarea parolelor se realizează prin selectarea tabului Passwords, click dreapta pe intrarea dorită, apoi selectarea opțiunii Send to Cracker. Parolele decriptate vor apărea în tabul Cracker (vezi fig. 7)

The passwords capture can be achieved by selecting the 'Passwords' tab from the bottom pane, right click on the desired entry and then choosing the 'Send to Cracker' option. The decrypted passwords will be shown in the 'Cracker' tab (see figure 7).

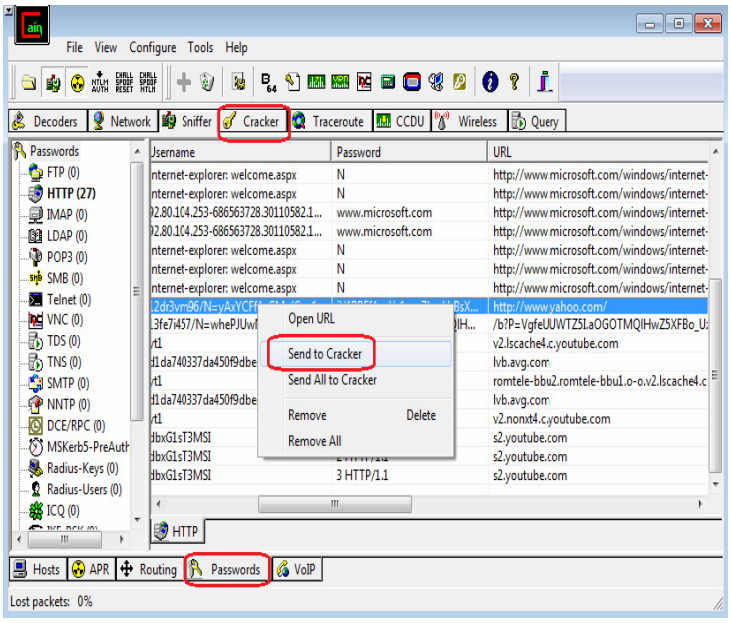

Fig 7. – Password decryption

Concluzii

Se poate observa cât de uşor de folosit este acest tip de atac – am avut nevoie doar de utilitarul Cain & Abel, dar totuşi este nevoie de acces în reţeaua locală. Acest tip de atac este greu de oprit deoarece speculează o breşă de securitate a unui protocol folosit pentru funcţionarea unei reţele bazată pe TCP/IP, dar poate fi prevenit. Una dintre metodele de prevenire a acestui tip de atac o reprezintă criptarea traficului. Dacă se foloseşte o criptare cu cheie partajată, se obţine un oarecare grad de securitate. În schimb, dacă se foloseşte o criptare fără cheie partajată şi fără autentificare, în care cheia de criptare se derivă prin schimbul de informaţii între cele două staţii, gradul de securitate este zero (atacatorul va stabili două canale de comunicaţie, cu fiecare dintre cele două staţi, şi chiar dacă acele canale sunt criptate, atacatorul are toate informaţiile necesare pentru decriptare). Pentru prevenirea unui atac de tip ARP poisoning trebuie monitorizat tot traficul ARP din reţeaua locală atât la nivelul dispozitivelor de interconectare folosind switch-uri ce implementeaza ARP inspection (interceptează şi validează cererile şi răspunsurile ARP), cât şi la nivelul staţiilor folosind programe de genul ARP Watch pentru a detecta eventualele schimbări în asocierile IP - MAC. În acelaşi timp, pentru destinaţiile importante (pt. gateway) se recomandă folosirea de asocieri statice în tabela ARP.

Bibliografie

1. Tanenbaum A., *Reţele de Calculatoare*, Ed. Byblos S.R.L., 2003.
2. Rughinis R., Deaconescu R., Ciorba A., Doinea B., *Reţele Locale*, Ed. Printech, 2009.
3. http://www.oxid.it/downloads/apr-intro.swf
4. http://en.wikipedia.org/wiki/ARP_spoofing
5. http://www.watchguard.com/infocenter/editorial/135324.asp

Conclusions

It can be seen how easily is to use this kind of attack (we only need the Cain & Abel utility), but still is required the access to the local network.

This type of attack is hard to stop because it speculates a flow in a network protocol, but it can be prevented.

One way to prevent this type of attack is the traffic encryption. If an encryption with a shared key is used, a degree of security is obtained. Otherwise, if it is used an encryption without a shared key and without authentication, where the encryption key is derived through the exchange of information between two stations, the security is zero (the attacker will establish two communication channels, one for each station, and even if those channels are encrypted the attacker has all the information necessary for decryption).

To prevent an ARP poisoning attack, all the ARP traffic from the local network must be monitored at the both level of interconnection devices using switches which implements the ARP inspection (intercepts and validates the ARP requests and answers), and also at the station level using programs like ARP Watch to detect the changes in the IP – MAC correspondence. At the same time, for the important destinations (gateway) is recommended to use static associations in the ARP table.

Bibliography

1. Tanenbaum A., *Retele de Calculatoare*, Ed. Byblos S.R.L., 2003.
2. Rughinis R., Deaconescu R., Ciorba A., Doinea B., *Retele Locale*, Ed. Printech, 2009.
3. http://www.oxid.it/downloads/apr-intro.swf
4. http://en.wikipedia.org/wiki/ARP_spoofing
5. http://www.watchguard.com/infocenter/editorial/135324.asp
6. http://packetstormsecurity.org/papers/general/Altering_ARP_Tables_v_1.00.htm